UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,	
-vs-	REPORT AND RECOMMENDATION
JOHN LOONEY,	22-CR-6009-CJS-MJP
Defendant.	

Pedersen, M.J. This matter is before the undersigned on defendant John Looney's ("Defendant") motion to suppress tangible evidence obtained from the search of his residence on the basis that the search warrant affidavit contained false information, or in the alternative, to hold a *Franks* hearing. (Napier Aff., Oct. 3, 2022, ECF No. 62.) Defendant made an additional motion to suppress evidence referenced in the government's notice of intent to use evidence on the basis that such evidence was obtained in violation of various federal privacy statutes. (Napier Aff., Feb. 24, 2023, ECF No. 72.) Following extensive briefing and oral argument, the undersigned recommends to the District Judge that no *Franks* hearing is necessary and that Defendant's motions to suppress be denied.

BACKGROUND

Defendant filed an omnibus motion containing 550 pages on October 5, 2022 (ECF No. 62). In it, Defendant sought a *Franks* hearing and suppression of evidence, among other prayers for relief. The government responded in opposition on October 19, 2022 (ECF No. 63). Defendant sought and was granted an adjournment of the oral argument date on October 26, 2022, December 5, 2022, and on January 20, 2023. On February 24, 2023, Defendant filed a motion to suppress based on allegations that the government violated federal privacy statutes (ECF No. 72). The parties argued the omnibus motion on February 27, 2023, and the undersigned reserved its decision related to Defendant's initial motion to suppress and request for a *Franks* hearing.

On March 14, 2023, the government filed its response in opposition to Defendant's suppression motion (ECF No. 74), and the undersigned heard oral argument on May 8, 2023. Based on the May oral argument, the undersigned set a further briefing schedule to ascertain whether a *Franks* hearing is required. (Minute Entry, May 8, 2023, ECF No. 76.)

Defendant and the government filed further papers in support of, and in opposition to, the suppression motions. All briefing was completed on August 11, 2023. On August 14, 2023, the undersigned heard oral argument on whether a *Franks* hearing should be scheduled.

Upon first review of the voluminous filings in this case, the undersigned was prepared to rule on the substantive issues raised concerning the operation of Freenet[1]. However, a careful reading of *Franks v. Delaware*, 438 U.S. 154 (1978), shows conclusively that the moving party has not met the requirements for entitlement to a *Franks* hearing. Thus, the undersigned cannot rule on the interesting and substantive issue regarding the operation of Freenet.

MOTION TO SUPPRESS TANGIBLE EVIDENCE

Defendant's arguments regarding a Franks hearing

In 2018 and 2019 Federal Bureau of Investigation ("FBI") Task Force Officer Carlton Turner was engaged in an investigation into Freenet, a peer-to-peer network, through which it was suspected that child pornography was being exchanged. (Gov't's Resp. at 1, Oct. 19, 2022, ECF No. 63.) During this investigation, Officer Turner observed requests for child pornography coming from the same IP address registered to Defendant's residence on three different occasions. (*Id.*) Officer Turner obtained a

[1] "Freenet is a distributed, decentralized alternative to the centralized World Wide Web, designed to unleash a new era of innovation and competition, while protecting freedom of speech and privacy." About Freenet, Introduction, available at https://freenet.org/about (last checked Aug. 14, 2023).

search warrant from the Hon. Marian W. Payson for Defendant's residence and, upon execution of that warrant, the FBI found three laptops, which contained over 1 million images and videos of child pornography. (*Id*. at 7.) In addition, the FBI found two thumb drives named after Freenet, which contained approximately 300 manifest keys[2] for child pornography files. (*Id*.)

The federal grand jury indicted Defendant on January 18, 2022, on three counts, charging him with possessing child pornography, in violation of Title 18, United States Code, Section 2252A(a)(5)(B) and (b)(2). (Indictment, ECF No. 36.) The government filed its notice of intent to use evidence on February 4, 2022, informing Defendant of its intention to use the evidence seized during the execution of the search warrant in the prosecution of this case. (Gov't's Resp. at 8, ECF No. 63.)

Defendant contends that he is entitled to a *Franks* hearing, arguing that the search warrant is defective because Officer Turner allegedly knowingly or recklessly made false statements in his affidavit in support of the search warrant that the Magistrate Judge relied upon in finding probable cause to issue the warrant. (Napier Aff. at 46, ECF No. 62.) More particularly, Defendant contends as follows:

> 46. The warrant affidavit uses a method, the Levine formula, to identify the downloader of files in the Freenet Network. This formula is designed

---

[2] The government uses the word "Network" to describe the peer-to-peer file sharing network at issues in this case—Freenet— and explains Freenet "manifest keys" as follows:

> Unlike other file sharing systems, the Network does not have a search function whereby users can search certain terms to locate files. Instead, the Network's software creates a unique key – a series of letters, numbers, and special characters – that is used to download any given file. Some of the keys contain words or phrases that describe the contents of the file. To download a file on the network [sic], a user must have the key for the file. A user who wishes to locate and download a file can obtain the key from: (a) a message board within the Network; (b) a website within the Network; or (c) another Network user. Once a user obtains the key associated with the file that he or she wants to download, the user must enter that exact key into the "download" box on the network's [sic] "file sharing" page."
>
> (Gov't's Resp. at 7–8 n.2.)

upon the even-share distribution of requests where requests are divided up evenly among the peers of the Suspect node. Based upon this division an expectation of how many requests would be received by a directly connected node, the FBI node, is determined [requests/peers]. The number of actual requests received by the FBI node is compared to the expectation and if it is close, the conclusion is made that the FBI node is actually connected to the Downloader. This is a totally false and reckless conclusion because 1) Freenet does not distribute requests in this even-share way, and 2) there are always some peers that are connected but not responding to requests because their queues are backed up, so the number of peers is not known. Because of this the percentage of even-share shown in the government spreadsheet cannot be calculated, and any even-share data is totally meaningless.

47. This is the basis of the government's conclusions, and everything follows from this false conclusion.

48. After setting aside the false and misleading material in the warrant affidavit the remaining information is insufficient to constitute probable cause. According to Franks, "in the event. . . the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause were lacking on the face of the affidavit.["] Id. at 154 After the exclusion of the aforementioned false information, the remaining information consists of the allegation that Defendant's computer sent requests for pieces of files to the FBI node. These pieces were less than 1% of the number of pieces required to download the files of interest and occurred so slowly that the only reasonable explanation was that the computer was only forwarding requests from another node. The Judge herein was not made aware of the importance of this timing, which indicates that the defendant was only relaying requests, although it was considered important in the Dickerman case. In addition, the normal operation of Freenet involves continually passing requests between nodes, regardless of content, and the user has no knowledge of or control over these requests.

49. With Freenet, requests are not evenly divided amongst the direct peers of the node, but instead are sent to nodes based upon routing algorithms which could send ALL requests to one peer or distribute unevenly to only a few of the peers. In addition, it is not possible to know which peers of a suspect node are sending and receiving requests even though the peers are 'connected'. These two fallacies, even-share and assumption that all peers are communicating, make it patently impossible to determine an expectation of the number of requests that

would be received by the FBI node and thereby identify the downloader of a file of interest.

50. The Affidavit states that the government has been investigating Freenet since 2011. "*Since approximately 2011, law enforcement has been investigating the trafficking of child pornography on the Network*." The Law Enforcement Freenet Project, known as the Black Ice project, focused on monitoring users on Freenet and collecting manifests and IP addresses in an attempt to provide a method to establish probable cause.

51. From the Black Ice Project: "*When a key is requested, first the node checks the local data store. If it's not found, the key's hash is turned into another number in the same zero to 1 range, and the request is routed to the node whose location is closest to the key. This goes on until some number of hops is exceeded, there are no more nodes to search, or the data is found (see figure 2). If the data is found, it is cached on each node along the path. So there is no one source node for a key, and attempting to find where it is currently stored will result in it being cached more widely*." [Exhibit G] **This is not even-share.**

52. It is not possible that the government does not know and understand how Freenet routes requests, even though in the Affidavit they repeatedly imply even-share routing, a totally FALSE routing description. In the Affidavit, the government uses Attachment C which includes Dr. Levine's M&M example, along with Officer Turners Fig. 1 and 2 example, plus the example provided in paragraphs 46-51 to demonstrate how Freenet routes requests. All these examples show that requests are distributed in an even-share manner, and are false and in no way relate to the actual operation of Freenet. The Black Ice Project disputes Freenet even-share routing. This shows a reckless disregard for the facts and a lack of Good Faith by the government. Accurate detailed descriptions of Freenet routing are provided in our attachments.

53. There is no evidence claimed against the Defendant to support probable cause other than falsely identifying the Defendants IP address as a result of misidentification as the Requestor of a FOI. The government has made **NO** claims that the Defendant has ever chatted, emailed, communicated, or contacted in any form or manner with anyone about child pornography. The government has made no claim that the Defendant ever shared any files with anyone else or made any files publicly available. The government has made no claim that the Defendant has ever associated with children of any age in any format either singly or in a group.

54. In this case, although the investigation by Officer Turner is described, it is very simple and faulty:

1. The modified FBI node collected data about the number of requests made for the FOI and provided a spreadsheet.

2. The additional data collected was the max and min number of pieces of the FOI required, the time required to collect the pieces, the number of peers, on average, connected, but not necessarily active, to the suspect node, and the IP address of the suspect node.

3. The 'even-share' was determined - blocks/peers. Then a calculation was made, peers*requests/blocks [69.2*69/12562 * 100 =38%] to determine how close the number of requests compare to the expected even-share of requests.

4. Although the actual number of requests received was 69, and the number of requests falsely expected from even-share was in the range (min and max) of 92.1 to 182, it was evidently enough to declare that the suspect node was the downloader of the file. Even though the number of requests was well outside the expected range.

5. This was repeated two more times.

6. At some point, before, after, or during the data collection, we don't know when, Officer Turner downloaded a FOI and verified it as child pornography. This raises the question, whether or not the FBI node requested any pieces of the files from the Suspect node, and if so, how many.

7. Finally, the IP address was used to identify the Defendant as the alleged downloader.

55. The only facts claimed by the government - a spreadsheet with data collected on three files. We have shown with numerous examples and references that the method used by Officer Turner, which calculates the even-share data is not valid and any conclusions are false. Common sense would indicate that downloading less than 1% [this was true on all three cases] of the data required is not sufficient to draw any conclusions, let alone establish probable cause.

56. In addition to providing false descriptions of Freenet routing of requests, other data was omitted from the affidavit. The conclusions reached by Officer Turner are based upon the faulty 'percentage of even-share' data, and shown in the spreadsheet GOV000320. The data is shown, but no information on what numbers would be necessary in order to reach a conclusion.

57. In the Dickerman[3] case, the government stated that a 100% value for percentage of even-share should be reached, and if it was less than a 100% "*we typically don't use those*".[Exhibit E] Only one file in this case reached 101% even after using the maximum number of peers and the minimum number of blocks for a worst case result. Officer Turner did not provide a threshold for the percentage of even-share data shown in the spreadsheet. This is the basis for the conclusion stated that the Defendant was the Downloader of the files and not simply relaying the requests from another node. This is like charging someone with a DWI without noting the blood alcohol level and through use of a method that does not match the reality of how one determines blood alcohol content.

58. The "facts" in the warrant affidavit have been shown to be **false** multiple times. The affidavit gave multiple examples of a false representation of the operation of Freenet, and repeatedly used references to a "peer reviewed" paper as proof of the accuracy of the method. We found no verification of these peer reviewers or a detailed description of exactly what was being reviewed. There was no independent verification of the formula used by the government. There was no indication that Levine or law enforcement ever asked the developers of Freenet [Exhibit F] to respond to the accuracy of the academic paper or method.[4]

59. The Government has omitted data or not provided relevant information in several areas. Every statement we have made is verifiable through multiple publicly available sources: academic papers, the actual publically [sic] available Freenet source code, or even from the law enforcement Black Ice Project.

To summarize, we have addressed the issues present in the warrant affidavit:

- We provided the actual method for routing requests within Freenet.
- We showed the false assumptions made by the Government.
- We showed through numerous calculations how choosing numbers that were realistic and typical made dramatic changes to the conclusions
- We showed that making requests is continuous and fundamental to the operation of Freenet.

[3] *United States v. Dickerman*, 954 F.3d 1060 (8th Cir. 2020).

[4]

> •We showed the configuration of the Freenet nodes, the Downloader, the Suspect, and the Observer [FBI], which would result in the data logged by the FBI, where the Defendant was not the Downloader, but only relaying the requests.
>
> •We showed the timing data herein being dramatically different in comparison to the Dickerman case.
>
> •We showed the threshold data from the Dickerman case, yet the warrant affidavit does not provide threshold data.

(Napier Aff. ¶¶ 46–59, ECF No. 62.)

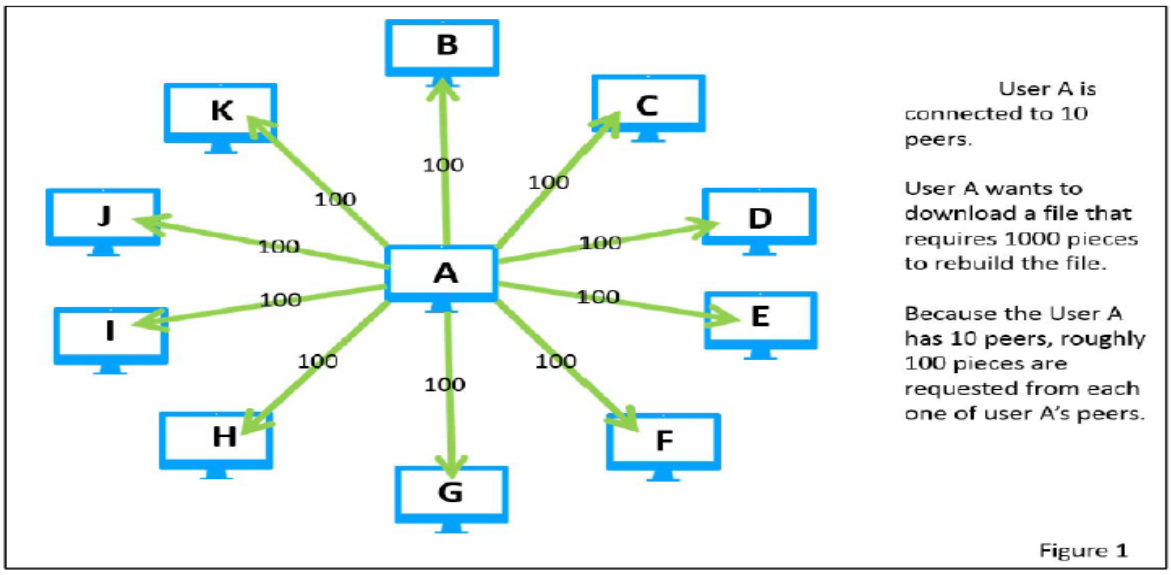
Moreover, in his submission dated April 2, 2023 (ECF No. 75), Defendant stated that the government provided him with an academic paper authored by Brian Levine in 2017, in support of the government's argument that Officer Turner's affidavit was factually accurate. In the paper, Mr. Levine stated, "when sending requests a node attempts to send it in the direction of the node closest to the block's location. Freenet **performs friend of a friend routing**." (James A. Napier letter to the Court at 1, Mar. 28, 2023, ECF No. 75.) Defendant argues that, "[t]his statement by Levine contradicts [ ] [Officer Turner's] Affidavit which stated '... relying on the fact an original or first level request is divided in approximately equally [sic] parts between each of the original requestor's peers and an intermediary or second-level request is subdivided evenly between the intermediary users' peers ...' ¶ 45 of Affidavit."

The letter does not indicate that Officer Turner was familiar with Mr. Levine's 2017 paper. Rather, it implies that because Mr. Levine's knowledge was the basis for Officer Turner's ability to conclude that Defendant was the requestor, not merely relaying another's request for files, and since Mr. Levine's 2017 paper contains an apparent internal inconsistency, then Officer Turner's affidavit must therefore be false. As discussed in detail below, this argument fails to meet the *Franks* standard for a hearing.

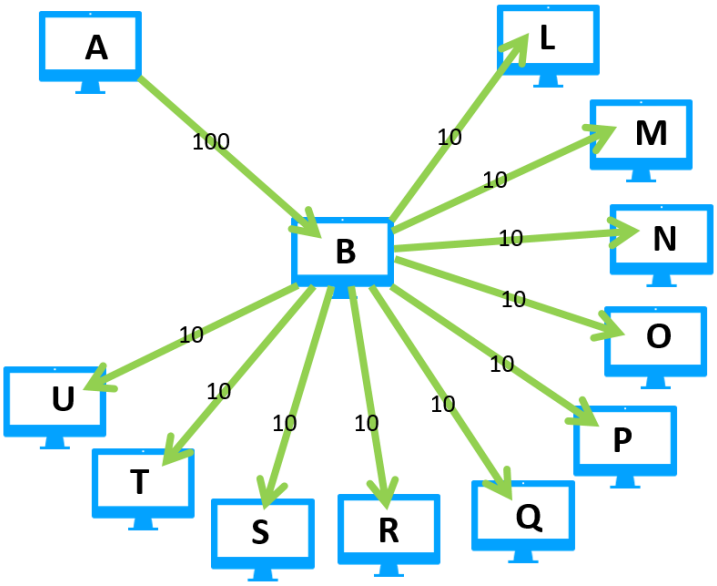
The government's arguments in opposition to a Franks hearing

In its papers in opposition to Defendant's assertions above, the government relies on Officer Turner's explanation of how Freenet operates, as follows:

> 8. When a user uploads a file into the Network, the software breaks the file into pieces (called "blocks") and encrypts each block.
>
> 9. The encrypted blocks are then randomly distributed and stored on individual users' computers throughout the Network.
>
> 10. In order for a file to be reassembled and downloaded, the software creates an index of all blocks necessary to reconstruct the file.
>
> . . .
>
> 15. When a user attempts to download a file, the Network first downloads the piece of the file containing the index, which provides the information required to retrieve the individual pieces of the file (i.e., the blocks). The Network software then requests all of the necessary blocks from the requesting user's peers. Rather than request all of the blocks from a single peer, the Network software divides the requests for blocks into roughly equal amounts among the requesting user's peers. If a user's peer does not have the particular block(s) being requested in its storage, that peer will then divide up the remaining requests and ask its peers for the block(s).
>
> 16. For example, if User "A" has 10 peers and requests 1000 blocks of a file, roughly 100 blocks are requested from each one of User A's peers. See Figure 1.



17. If Peer "B" receives User A's request for 100 blocks of the file, but does not have any of those blocks in its storage, Peer B forwards on the requests to Peer B's peers. If Peer B has 10 peers of its own, roughly 10 blocks are requested from each one of Peer B's peers. See Figure 2.



Peer B receives user A's request for 100 pieces of the file. Peer B does not have any of the pieces in its storage.

Peer B forwards on the request for pieces to each one of its peers.

Because B has 10 peers, roughly 10 pieces are requested from each one of B's peers.

Figure 2

31. A modified version of the Network software is available to sworn law enforcement officers to assist in conducting Network investigations. I have been trained on the operation of the modified law enforcement version of the Network.

. . .

33. The information logged by law enforcement includes, but is not limited to: the IP addresses of the law enforcement computer's peers; the number of peers those peers report to have; a unique identifier assigned by the software (referred to as the computer's Network "location"); the remaining number of times a request for a piece of a file may be forwarded; the date/time of requests received from a peer; and the digital hash value of a requested piece.

. . .

43. Your affiant has reviewed a peer-reviewed, published, and publicly available academic paper that describes the methodology behind this mathematical formula.

44. In basic terms, the formula uses three known variables—(a) the approximate minimum and maximum number of blocks the original requestor could request, in total, from its peers; (b) the number of blocks

requested from the law enforcement computer; and (c) the number of peers the requesting computer has—and one assumption—(d) that the original requestor (if it is not the computer directly connected to the law enforcement computer) has 8 peers.[5]

45. Then, relying on the fact that an original or first-level request is divided in approximately equally [sic] parts between each of the original requestor's peers and an intermediary or second-level request is subdivided evenly between the intermediary user's peers (*see* Figures 1 and 2), the formula determines whether it is more probable than not that a request received by a law enforcement computer for a specific number of blocks of a known "file of interest" was received from an original requestor or a mere intermediary.

46. For example, assume File of Interest A requires a minimum of approximately 6,000 blocks to download. An initial request could seek anywhere from approximately 6,000 to 12,000 blocks to download this file.

47. The law enforcement computer receives a request for 100 blocks of File of Interest A from User X. Through the request, law enforcement is also informed that User X has 50 peers and that the request can be forwarded 18 times.

48. If User X were the original requestor, then a recipient of a request from User X would expect to receive a request for somewhere between **120 blocks** (6,000 minimum necessary blocks/50 peers) and **240 blocks** (12,000 maximum necessary blocks/50 peers).

49. If, in the alternative, User X were a second level requestor, then User X likely received a request from the original user for anywhere from 750 blocks (6,000 minimum required blocks/8 peers) to 1,500 blocks (12,000 maximum required blocks/8 peers). A recipient of a second-level request from User X would then expect to receive a request for anywhere from approximately **15 blocks** (750 requested blocks/50 peers) to **30 blocks** (1,500 blocks/50 peers).

---

[5] The formula assumes that, in a scenario where the law enforcement computer is two degrees of separation from the original requestor, the original requestor has 8 peers. This is a very conservative estimate because the average user has significantly more than 8 peers. As a result, the formula will underestimate the likelihood that a request is received from an original requestor; this conservative assumption will identify fewer actual original requestors than actually exist. (Turner Aff. ¶ 44, ECF No. 62-1.)

50. Note that the number of requests the law enforcement computer receives if User X is an original requestor is substantially larger (often by a factor of 10) than the number of requests the law enforcement computer would receive if User X were merely a second-level or intermediary requestor.

51. In this example, the law enforcement computer received a request for 100 blocks. That request falls much closer to the expected range for an original request from User X (120-240). In contrast, a request for 100 blocks is substantially greater than the expected range for a second level request from User X (15-30 blocks). Therefore, there is a high probability that User X was the original requestor of File of Interest A.

. . .

52. The peer reviewed and published academic paper referenced above contains a detailed evaluation of this methodology and concludes that the formula is highly accurate in differentiating original requestors from second-level/intermediary requestors.

53. Specifically, the authors of this paper tested the formula using over 26,000 test runs. In those test runs, the formula has an approximately 2% false positive rate (i.e., it misidentified an intermediary requestor as an original requestor only 2% of the time).

54. Based upon my training and experience, I believe this to be a reliable method to determine whether it is significantly more probable than not that that a given computer using the Network is the original requestor of a file of interest.

. . .

55. I am also aware through my training and experience that dozens of searches of digital devices have been conducted by law enforcement officers (either through court-authorization or consent) related to targets whose IP addresses were identified based upon analysis of information from the Network's law enforcement computers, pursuant to which evidence of child pornography possession was located.

56. Further, search warrants issued on the basis of the above-described formula have consistently withstood judicial scrutiny on a motion to suppress. As an example, enclosed herewith as **Attachment C** is a decision from Magistrate Judge Nannette A. Baker, Easter District of Missouri, in the case entitled denying a defendant's motion to suppress a search warrant obtain on the basis of this formula.

(Gov't's Resp. at 2–7 (quoting Turner Aff., Feb. 21, 2019, ECF No. 62-2), ECF No. 63.)

The government further contends that "[t]he defense has offered zero evidence to undermine the accuracy of the Formula's[6] prediction." (Gov't's Resp. at 14.) Instead, the government asserts that Defendant "has submitted nothing more than a collection of documents printed from the internet that theorize the Formula should not work," but that Defendant has not provided any evidence that the articles on which it relies were peer reviewed or any affidavit from the authors of the articles in support of his motion for a Franks hearing. (Id. at 14–15.)

Defendant's arguments regarding privacy statutes

Defendant also moves to suppress tangible evidence contained in the government's notice of intent to use evidence (Napier Aff. at Ex. A, ECF No. 72-2) on the grounds that the government purportedly violated various federal privacy statutes. (Napier Aff. ¶ 6, ECF No. 72.) Indeed, Defendant asserts that since he was "using Freenet in the privacy of his home on a pass-word [sic] protected computer, [ ] he had a reasonable expectation of privacy." (*Id.* ¶ 7.) Particularly, Defendant contends that the government violated the following:

1. Stored Communication Law[7] – Defendant contends that the modified version of Freenet utilized by law enforcement enabled it to "tap into information transmitted over wire and extract it for logging . . . the software program fits the definition of a *wiretap*." (*Id.* ¶ 9.) Defendant contends that since Officer Turner did not obtain court authorization for a wiretap he violated 18 U.S.C. § 2511. (*Id.*) Defendant further argues that

> 12. Since Freenet provides a private electronic (wire) file transfer service to the public, no one, including the provider of a communication service,

[6] The government defined "Formula" as the explanation provided in Officer Turner's affidavit for how "information was put into a mathematical formula [ ] to determine whether a particular device was attempting to download child pornography." (Gov't's Resp. at 4.)

[7] Defendant is referring to the Stored Communications Act ("SCA"), 18.U.S.C. §§ 2701–13.

> can monitor network traffic or content transmitted through the network. The exception for monitoring is quite strict," ... *a provider of wire communication service to the public* ***shall not utilize service observing or random monitoring*** *except for mechanical or service quality control checks."* 18 U.S. Code § 2511(2)(a)(i) (emphasis added).

(*Id.* ¶ 12.)

2. Interception Law[8] – Defendant argues as follows:

> 15. Files transmitted are broken into smaller blocks for transmission. Hash code calculators are designed to check for transmission errors of a block. Each byte within a block is crunched through a formula to produce a hash code. After transmission, the same formula is applied. If the hash codes do not match, the block must be retransmitted.[9] However, law enforcement has found that hash codes can be used in other creative ways to bypass pen register, interception, and stored communication laws. Hash codes can be used to identify child pornography downloaded to specific remote computers. Using hash codes from a stored communication system for a purpose other than checking for transmission errors (its designed intent) also exceeds the authority granted to general users to access the facility. 18 U.S. Code § 2701.
>
> 16. Law enforcement used hash codes to uniquely identify content transmitted. {Affidavit #61(f)}. "Content" of an electronic communication is defined to include *"any information concerning the substance, purport or meaning of that communication;"* 18 U.S. Code § 2510(8). Officer Turner obtained the hash codes so they can be used to verify content. {Affidavit #33, 61(f), 62(f), 63(f)} However, Officer Turner had no court authorization to intercept content pursuant to 18 U.S. Code § 2516. Officer Turner obtained this content by running his special modified version of the Freenet software. "Intercept" simply means to acquire the content of an electronic communication through the use of any electronic, mechanical or other device. 18 U.S. Code § 2510(4). So, Officer Turner intercepted three hash codes without any Court authorization to do so, in violation of 18 U.S. Code § 2511(1)(a).
>
> 17. The three intercepted hash codes were disclosed in the affidavit in violation of 18 U.S. Code § 2511(1)(c). The three intercepted hash codes are being used to prosecute the Defendant, in violation of 18 U.S. Code

---

[8] The statute implicated by this argument is the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2510–23.

[9] BitTorrent.org. *For Developers.* http://www.bittorrent.org/beps/bep 0005.html Accessed January 14, 2019.

> § 2511(1)(d). Any intercepted communications and evidence received in violation of the chapter may not be received in evidence and should be suppressed. 18 U.S. Code § 2515.
>
> 18. The second category of *"content"* Officer Turner obtained was the report of the probability formula used to predict what content was being transmitted and which user downloaded it. The meaning of *"content"* includes *"any information concerning the substance, purport or meaning of that communication;"* Since the formula can, allegedly, predict with 98% accuracy the substance, purport and meaning of a communication(down loader v. relayor [sic]), its report qualifies as content. Yet, Officer Turner did not obtain prior authorization to intercept content using this method, 18 U.S. Code § 2516. Therefore, running this program to obtain reports of content transmitted without any prior court authorization violates 18 U.S. Code § 2511(1)(a).

(*Id.*)

3. Electronic Surveillance – Defendant contends that Officer Turner was not a party to any Freenet conversation, instead utilizing software to conduct surveillance and argues that

> 22. **Electronic Surveillance** means acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a nonelectronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.
>
> 23. The meaning of *person* means *"every infant member of the species homo sapiens who is born alive and at any state of development,"* 1 U.S. Code § 8. Officer Turner had a software program monitoring the communications (a modified version of Freenet). Software does not qualify as a *person* who can be party to a conversation. As such, this software program is not a *person* but a *thing*. Therefore, Officer Turner was conducting Electronic Surveillance using a *thing* (wiretap software) to monitor private communications without a warrant. Since software programs are not people, they cannot grant permission for someone else to record (or log) what is being communicated. EO-12333 was codified into law in the 1986 Electronic Communications and Privacy Act, which prohibits wiretapping without a warrant, 18 U.S. Code § 2511, 18 U.S. Code § 2701, and 18 U.S. Code § 3121.

(*Id.*)

4. Pen Register Law[10] – in this respect Defendant contends that

24. Freenet works to preserve the anonymity of its users. {Affidavit #5, 6} Yet Officer Turner used the modified version of the Network to extract IP addresses with a probability of having downloaded suspicious content. These IP addresses were logged. Officer Turner then went through a long process of submitting various administrative subpoenas to obtain the identity of the owner for the IP address. {Affidavit #68-69}. The name returned from these subpoenas was written on the request for an arrest warrant, and the resulting address was written on the request for a search warrant. However, Officer Turner did not obtain a warrant before beginning the process of unmasking the identity of the end user, violating 18 U.S. Code§ 3121. The requirement for a warrant is explicitly stated in 18 U.S. Code§ 2703(c)(l)(A).

> **(1)** A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity-
>
> **(A)** obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure ... (emphasis added)

25. A pen register is not just a device, but also a "process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." Use of a pen register process requires a warrant, 18 U.S. Code § 3121.

26. Officer Turner gives a detailed explanation of the route taken for a file block request. Once located, the file block would be returned along this same route. Officer Turner describes how a request goes out from User A to User B. If User B does not have the requested block, the request is forwarded to another user, say User M, and this request is forwarded up to 18 times. {Affidavit #15-17}. This route assists law enforcement to distinguish between a user that is the original requestor and one that has forwarded the request. {Affidavit #18}. The modified version of the software automatically logs this routing information and the number of times a request may be forwarded. {Affidavit #32-33}. However, any device or process which records routing information

[10] Defendant is referring to the Pen Register and Trap and Trace Statute ("Pen Register Act"), 18 U.S.C. §§ 3121–27.

> cannot be used unless a pen register warrant is obtained, for a pen register protects routing information. 18 U.S. Code § 3121. Since no such warrant was obtained prior to using this logging program, all information derived from this log should be suppressed.

(*Id.*)

> 5. Intent – Defendant argues that
>
> 29. As part of the user Freenet user agreement, the user agrees to provide Freenet a portion of the user's disk space to Freenet. {Affidavit #7} Free net then will store whatever the system deems necessary to store there for efficient network operation, randomly distributing them on various user's computers. {Affidavit #9}. Data is put on the user's computer, even if the user did not request it:
>
> > *"Unlike other peer-to-peer networks, you as* a *user have little or no control over what is stored in your datastore. Instead, files are kept or deleted depending on how popular they are. This allows Freenet to be censorship-resistant. There is no "delete file" operation*[11].
>
> 30. The Affidavit's simplistic wagon-wheel diagrams of the network gives the impression that users have knowledge of their directly connected nodes. A more accurate representation of any such network is a highway map of the country. Baltimore and Denver are on the same 1-70, but you cannot drive between them without stopping. Files transmitted between these two cities will probably have an intermediate transmission point. There are large highways and small residential streets, but both are able to handle vehicle traffic at different capacities. If someone purchases a home on a quiet, residential street, they do not expect a parade of tanker trucks to flow in front of their home. Yet, if there is a major crash on the nearby freeway, traffic will be diverted onto their street to balance the traffic load. Similarly, if a user downloads Freenet for legitimate purposes, he has no control over what network balancing algorithm may decide to put on his computer's disk space. The Freenet algorithms add or delete files from the disk space according to the popularity of that file with others in the network and the transmission route between sender and receiver, not because the said user requested the file. Therefore, if a forensic search of a computer with Freenet finds a file, or file block, without any indication the user

[11] Freenetproject.org, Freenet Documentation, https://freenetproject.org/pages/documentation.html, Accessed January 2, 2023.

> requested it, i.e., a relayer, this lacks criminal intent that the user himself download the file.

(Id.)

6. Modified Versions of Freenet are not Publicly Available – Finally, Defendant contends that

> 31. Officer Turner has implied that this modified version of Freenet built by law enforcement should be considered publicly available because Freenet source code is publicly available on a website. {Affidavit #6} Only software engineers can understand software, and only those with nefarious purposes would download this source code and modify it to do what law enforcement has done here - monitor network traffic to predict content transmitted. In order for something to be considered "publicly available", the information must be available to any member of the general public[12] Note that this definition requires that the information, not just source code that is unintelligible to the average person, must be available to the general public. Therefore, the modified Freenet not publicly available, so it requires a warrant to use. Since no warrant was obtained prior to use, it was used in violation of laws defined in the Electronic Communications and Privacy Act of 1986.

(*Id.*)

The government's arguments in opposition to the alleged violation of the privacy statutes.

The government contends that Defendant did not have any expectation of privacy in the requests made over the "Network" and, therefore, Officer Turner did not engage in any search when he observed and recorded information voluntarily disclosed by Defendant. (Gov't's Resp. at 6–7, ECF No. 74.) More specifically, the government asserts that when Defendant utilized the Network, he voluntarily turned over his IP address and hash value of the requested file to his peers.[13] (*Id.* at 4.) In

[12] Office of Director of National Intelligence (DNI), *Civil Liberties and Privacy Guidance for Intelligence Community Professionals: Properly Obtaining and Using Publicly Available Information* (July 2011), *at 3 #1.*

[13] In his reply, in which Defendant makes many of the same arguments as contained in his original motion to suppress based upon Officer Turner's alleged violations of privacy *(continued)*

addition, the government contends that Officer Turner explained that the types information that law enforcement logged is available to anyone using the standard Network. (*Id*. at 6.) For these reasons, the government contends that Defendant "cannot invoke the protections of the Fourth Amendment." (*Id*. at 7.)

The government further contends that the ECPA is not applicable because an exception states,

> "it shall not be unlawful [] for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communications has given prior consent to such interception." 18 U.S.C. § 2511(2)(c). This exception permits undercover law enforcement officers and confidential informants to engage in consensual wire communications with a target without obtaining a warrant.

(*Id*.) The government asserts that Officer Turner's actions fall under the exception because he was a party to the exchanges, was acting in an undercover capacity, and was connected to Defendant's computer as a peer when he obtained the information at issue as result of Defendant's requests for child pornography. (*Id*.) In addition, the government asserts that Defendant failed to establish that the information Officer Turner collected constituted a "wire, oral, or electronic communication" under the ECPA, arguing that the information was more like recording the characteristics of a message as opposed to the contents of the message. (*Id*. at 8.)

With respect to the argument that Officer Turner's receipt of Defendant's requests violated the SCA, the government responds as follows:

> The Stored Communications Act prohibits "intentionally access[ing] without authorization a facility through which an electronic communication service is provided . . . and thereby obtain[ing] . . . a wire or electronic communication while it is in electronic storage." 18 U.S.C. § 2701.

---

statutes, he contends that "[r]egular users never see hash codes – they are not publicly available." (Napier Aff. ¶ 34, ECF No. 78.)

> The SCA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. §§ 2711(1) and 2510(17).
>
> The SCA also contains an exception for "a user of [a wire electronic communications] service with respect to a communication of or intended for that user." 18 U.S.C. § 2701(c)(2).

(*Id.* at 8.) The government raises several arguments in opposition to Defendant's assertions, contending that Defendant:

> has not established that the Network meets the definitions of a "facility through which an electronic communication service is provided." Second, he has not established that his requests constitute "communications." Third, even if the requests constituted communications, they were not stored communications; they were active requests directed at Ofc. Turner. Fourth, the defendant voluntarily transmitted his requests to all his peers, including Ofc. Turner. As such, the exception under 18 U.S.C. § 2701(c)(2) applies.

(*Id.* at 9.) In addition, the government explains that 18 U.S.C. § 2703(c)(2) "expressly permits law enforcement to obtain subscriber information from an electronic commination [sic] service or remote computing service provider with a subpoena" such that law enforcement did not violate the SCA by obtaining information related to Defendant's IP address by subpoena. (*Id.*) Finally, the government argues that the sole remedy for a violation of SCA is a civil action for damages (and criminal punishment in certain circumstances), not suppression of evidence, citing 18 U.S.C. § 2708. (*Id.*)

With respect to Defendant's allegations that the government violated the Pen Register Act, the government explains that "The term 'pen' means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted. 18 U.S.C. § 3127(3)." (internal quotations omitted) (*Id.* at 10.) It further explains that Defendant is incorrect in asserting that his IP address

constitutes "routing information" because Officer Turner only obtained the IP address from a computer from which he received a request and case law provides that "[a] single IP address that is voluntarily transmitted from one computer to another is not covered by the Pen Register Statute." (*Id.*) In addition, the government argues that suppression is not the remedy for any alleged violation of the SCA, but rather that the proper remedies are civil actions and/or criminal charges. (*Id.* at 11.)

Finally, the government asserts that the good faith exception to the exclusionary rule should apply to Officer Turner's actions as he "clearly acted in good faith when, while operating in an undercover capacity on the Network, he received the requests for child pornography files from the defendant and the information associated with those requests." (*Id.*)

STANDARD OF LAW

The District Judge referred this case to the undersigned per 28 U.S.C. § 636(b)(1)(A) and (B) to hear and determine pretrial matters and to submit a report and recommendation on any motion to suppress. (Text Order of Referral, ECF No. 38.)

The Affidavit From Officer Turner Provides Probable Cause

This case involves evidence derived from Freenet that led investigators to conclude that Defendant's computer had requested child pornography files.

Defendant has not established his entitlement to a Franks hearing nor has he met the requirement to make "a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit…."[14]

Not only does Defendant argue that the search warrant affidavit did not provide probable cause for searching his computer, he also contends that the affiant,

[14] *Franks,* 438 U.S. at 155–56.

Officer Turner, knowingly and intentionally, or with a reckless disregard for the truth, included false statements about the manner in which Freenet operates.

In the *Franks* decision, the Court set out the standard by which an accused could challenge the contents of an *ex parte* search warrant affidavit. In so doing, it reversed a ruling from the Delaware Supreme Court that held one could never challenge the veracity of a search warrant affidavit. However, the Court set out the burden on the defense to entitle it to a hearing:

> we hold that, where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request. In the event that at that hearing the allegation of perjury or reckless disregard is established by the defendant by a preponderance of the evidence, and, with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit.

Franks, 438 U.S. at 155–56. In its discussion of the holding, the Court stated, "the rule announced today has a limited scope, both in regard to when exclusion of the seized evidence is mandated, and when a hearing on allegations of misstatements must be accorded." *Id*. at 167. In answer to arguments by the state that a hearing would diminish the importance of the process to obtain a warrant, the Court answered, "allowing an evidentiary hearing, *after a suitable preliminary proffer of material falsity*, would not diminish the importance and solemnity of the warrant-issuing process." *Id.* at 169 (emphasis added). Justice Blackman then wrote the following concerning the burden on Defendant to obtain a hearing:

> To mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine. There *must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be*

> *accompanied by an offer of proof. They should point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a* statement *of supporting reasons. Affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained.* Allegations of negligence or innocent mistake are insufficient. The deliberate falsity or reckless disregard whose impeachment is permitted today is only that of the affiant, not of any nongovernmental informant. Finally, if these requirements are met, and if, when material that is the subject of the alleged falsity or reckless disregard is set to one side, there remains sufficient content in the warrant affidavit to support a finding of probable cause, no hearing is required. On the other hand, if the remaining content is insufficient, the defendant is entitled, under the Fourth and Fourteenth Amendments, to his hearing. Whether he will prevail at that hearing is, of course, another issue.

Franks, 438 U.S. at 171–72 (emphasis added).

In a recent decision, the U.S. Court of Appeals for the Second Circuit wrote about the burden of a "substantial preliminary showing":

> We have recognized that *Franks* "adopted the substantial preliminary showing requirement and stressed the need for a 'sensible threshold' before a hearing would be required" to alleviate concerns that "frivolous challenges" could result in "unnecessary pretrial delays." *United States v. Figueroa*, 750 F.2d 232, 237 (2d Cir. 1984) (quoting *Franks*, 438 U.S. at 170, 98 S. Ct. 2674).
>
> Reflecting this purpose, courts have construed the burden imposed by the "substantial preliminary showing" standard as a heavy one that requires more than a mere conclusory showing. This includes our Circuit, several of our sister circuits, and the district courts within our Circuit. As such, the substantial preliminary showing standard imposes a "high" burden on Sandalo.

United States v. Sandalo, 70 F.4th 77, 85–86 (2d Cir. 2023) (footnotes omitted). In *Sandalo*, the Court also stated: "But even if the statement was false, we are not persuaded that this suggests the Officers knew the statement was false." *Id.* at 89. This is precisely the basis on which Defendant's proffers fail.

Turning to the case here, Defendant has failed to meet his burden to be entitled to a hearing under the *Franks*' standard as he has not provided any sworn testimony

that the evidence contained in Officer Turner's affidavit is false nor has he attempted to explain the absence of "affidavits or sworn or otherwise reliable statements of witnesses." *Franks*, 438 U.S. at 171; *see United States v. Orozco–Prada*, 732 F.2d 1076, 1089 (2d Cir. 1984) (affirming denial of *Franks* hearing on grounds that defendant "made no offer of proof and did not submit a sworn or otherwise reliable statement of a witness."); *United States v. John Rivera-Banchs*, 516 F. Supp. 3d 316, 323 (W.D.N.Y. 2021) (denying *Franks* hearing where "Defendant [did] not even come close to meeting [the] high burden" set forth in *Franks*.); *United States v. Dupree*, 781 F. Supp. 2d 115, 144–46 (E.D.N.Y. 2011) (denying defendants' request for a *Franks* hearing where the defendants' assertions were not supported by an offer of proof, such as an affidavit from a witness with personal knowledge or an otherwise reliable witness statement, because the defendants did not set forth any legal support for their contention that an omission from the warrant application required a *Franks* hearing); *United States v. Taylor*, 672 F. Supp. 2d 539, 540–41 (S.D.N.Y. 2009) (denying defendant's request for a *Franks* hearing where his initial *Franks* showing consisted of a "sparse, half-page affidavit and [an] ... assertion in a memorandum of law" to demonstrate recklessness by the FBI agent issuing the search warrant for the defendant's apartment).

In fact, Defendant has not provided any sworn testimony other than that of his attorney regarding the operation of Freenet and his attorney does not have first-hand knowledge about this information, rendering his affidavit insufficient to warrant a *Franks* hearing. It is settled law that a motion seeking a [ ] hearing must be accompanied by an affidavit from someone having personal knowledge of the facts justifying the hearing. *United States v. Rivera-Figueroa*, No. 17CR00183LJVJJM, 2018 WL 7291428, at *15 (W.D.N.Y. Aug. 21, 2018), report and recommendation adopted, No. 17-CR-183, 2019 WL 244490 (W.D.N.Y. Jan. 17, 2019) (citing *United States v. Gillette*, 383 F.2d 843, 848–49 (2d Cir. 1967) ("[t]he affidavit submitted for

appellant is insufficient in that it does not ... allege personal knowledge on the part of appellant's attorney; accordingly, there was no factual issue to be resolved and the denial of a hearing was correct")).

In addition, Defendant has alleged that the entirety of Officer Turner's explanation concerning how Freenet works and how the FBI was able to determine that Defendant's computer was the one requesting the file is false. Defendant has submitted scholarly papers and referred to other cases[15] attempting to show that Officer Turner must have known that his explanation was false. What is missing, however, is any evidence that Officer Turner was aware of that information and recklessly disregarded it, or knowingly used false information to persuade the magistrate judge to issue the warrant. Again, "those allegations must be accompanied by an offer of proof," and "[a]ffidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained." The academic papers cited by Defendant are not sworn statements and even if they were, Defendant has not shown that Officer Turner could or should have been aware of them at the time he completed the application for the search warrant and obtained the warrant from Judge Payson.

---

[15] For example, Defendant cites to the following scholarly papers: Stephanie Roos, *Measuring Freenet in the Wild: Censorship-resilience under Observation*, undated (Napier Aff. at Ex. C, ECF No. 62-2); Todd Baumesiter, *et al.*, *A Routing Table Insertion (RTI) Attack on Freenet*, Sept. 18, 2012 (*Id.* at Ex. C, ECF No. 62-3); Ian Clarke, *et al.*, *Freenet: A Distributed Anonymous Information Storage and Retrieval System*, undated (*Id.* at Ex. D, ECF No. 62-4); Freenet Project, Inc., *The discredited Levine 2017 approach is still used*, Aug. 28, 2022 (*Id.* at Ex. F, ECF No. 62-6); Wayne Becker, *et al.*, *Black Ice: The Law Enforcement Freenet Project*, Sept. 4, 2013 (*Id.* at Ex. G, ECF No. 62-7); Freenet Project Inc., *Statistical results without false positives check are most likely wrong*, Sept. 9, 2019. (*Id.* at Ex. G, ECF No. 62-8.)

In addition, Defendant cites to an application for a search warrant from a Southern District of New York case, *United States v. Corbett*, which had search warrant magistrate number 20-MAH-669 and eventually was assigned criminal case number 20-CR-525. (Napier Aff. ¶ 2 & Ex. A, ECF No. 78-1.) Defendant also cites to cases he refers to as "*McF*" and "*Case X*," which he asserts proves that Freenet does not use even share. (Def.'s Memo in Preparation for Aug. 14, 2023, oral arguments at 10–11, ECF No. 86.)

At oral argument, defense counsel submitted excerpts purporting to be from a case that pre-dated the search warrant affidavit here. He identified the case only as *McF*. Those excerpts do not amount to sworn testimony, and the explanation for excluding the name and further information about the case is that the defense counsel for *McF* did not have permission from his client to provide that information. Once again, even if the excerpts *were* verified, Defendant has not made a showing that Officer Turner was aware of the information and the questions arguably raised by the excerpts.

Defendant has failed to make "a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit...." Instead, Defendant has demonstrated a "mere desire to cross-examine." *Franks*, 438 U.S. at 171. Having not met the requirements set forth in *Franks*, he is not entitled to a hearing to cross-examine Officer Turner about other theories of how Freenet works, or the officer's experience with other cases involving Freenet and the identification of a requesting node.

PRIVACY ISSUES

Fourth Amendment

Based upon the representations contained in Officer Turner's affidavit in support of the search warrant, the undersigned finds that Defendant did not have a reasonable expectation of privacy in the information gathered by Officer Turner such that Fourth Amendment's protections would be implicated. Defendant requested information from Officer Turner—a peer—and, therefore voluntarily provided his IP address and hash value of the file he was requesting to Officer Turner. Defendant's counsel's assertion that "[r]egular users never see hash codes – they are not publicly available" is not supported by any evidence. (Napier Aff. ¶ 34, ECF No. 78.) In any

event, as a logical matter, a request would not work without the requestor providing the IP address and the hash; without the hash the recipient computer would not know what part of a file the requestor seeks. Simply because the public may not "see" this information does not mean that it is not publicly available. This is akin to caller I.D. where one home may have that technology and can decipher the phone number from which the call originated versus a home that does not have caller I.D. technology and cannot see the phone number. Simply because the home without the caller I.D. technology cannot see the phone number does not mean that the information was not *available to be seen*. For these reasons the undersigned recommends that the District Judge deny that portion of Defendant's motion to suppress (ECF No. 72), which asserts that the government violated the Fourth Amendment.

The Electronic Communications Privacy Act[16]

Defendant asserts that the government violated this statute because it did not obtain court authorization for a wiretap. However, the government plausibly explained that an exception applies under 18 U.S.C. § 2511(2)(c), which provides: "(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception." Here, Officer Turner was acting in an undercover capacity and was a party to the conversation since he was connected to Defendant's computer as a peer because of Defendant's alleged request for child pornography. Under these circumstances, the undersigned recommends to the District Judge that Officer Tuner's actions fell squarely within the exception and that, therefore, suppression is not warranted.

[16] Defense counsel refers to this as "Interception Law" in his affidavit. (Napier Aff. ¶ 13, ECF No. 72.)

Stored Communication Act

Defendant contends that Officer Turner violated the SCA because he utilized modified software to "tap into information transmitted over wire and extract it for logging," and, therefore, his actions were akin to a wiretap. Defendant contends that he did not voluntarily provide any information to Officer Turner, but rather that Officer Turner extracted such information via "wiretap software." For these reasons, Defendant argues that Officer Turner was required to obtain court authorization prior to extracting such information. In addition, Defendant contends that the manner in which Officer Turner utilized Freenet exceed the authorized use of that program because the general public did not have the same access as Officer Turner.

The undersigned agrees with the government that the SCA does not apply. The SCA contains an exception for "a user of [a wire electronic communications] service with respect to a communication of or intended for that user." 18 U.S.C. § 2701(c)(2). The undersigned finds that this exception applies here as Officer Turner received a voluntary request from Defendant.

Moreover, the SCA prohibits "intentionally access[ing] without authorization a facility through which an electronic communication service is provided . . . and thereby obtain[ing] . . . a wire or electronic communication while it is in electronic storage." 18 U.S.C. § 2701. While the government asserts that Defendant has failed to establish that the requests qualified as a "communication," it argues that even if Defendant had established this, the communications at issue here were not "in electronic storage," but rather were active requests. The undersigned agrees with the government that the SCA does not apply to the present situation for this reason.

In addition, Defendant contends that Officer Turner improperly determined the owner of the IP address at issue by submitting subpoenas to obtain that information when he was required to obtain a warrant prior to beginning the whole process of finding the owner of the IP address. However, the government explained

that 18 U.S.C. § 2703(c)(2)[17] expressly permits law enforcement to obtain information regarding IP addresses via subpoena.

Finally, even if the undersigned adopted wholesale all of Defendant's arguments, it would still not recommend that suppression is warranted because the only remedies for a breach of the SCA is a civil action for damages or, in certain circumstances, criminal repercussions. For all of the forgoing reasons, the undersigned recommends that the District Judge deny that part of Defendant's motion seeking suppression of the information obtained by Officer Turner.

Pen Register Act

Defendant asserts that Officer Turner violated the Pen Register Act because he obtained Defendant's "routing information" and such information cannot be obtained without a warrant. Defendant concludes that since Officer Turner did not obtain a warrant that suppression of any logs of routing information is warranted. However, the government explains that the Pen Register Act does not apply to a single IP address obtained by a computer as a result of that computer receiving a request. The government cites to *Capitol Rec. Inc. v. Thomas-Rasset*, No. CIV 06-1497(MJD/RLE), 2009 WL 1664468, at *3 (D. Minn. Jun. 11, 2009), which explains that the Pen Register Act does not prevent the recording of IP addresses associated with communications sent to a person as IP addresses are required for computers to be able to communicate with each other.

Even if the undersigned credited all of Defendant's arguments, like the SCA, suppression is not an available remedy for a violation of the Pen Register Act. Based upon the forgoing, the undersigned finds that the Pen Register Act is not applicable

[17] 18 U.S.C. § 2703(c)(2) provides, in sum and substance, that a government entity is not required to obtain a warrant to obtain certain information, including an address, from a provider of an electronic communication service or remote computing service, and instead can utilize a subpoena.

here and recommends that the District Judge deny that portion of Defendant's motion seeking to suppress in this respect.

To the extent Defendant has made any other arguments that suppression is warranted based on a violation of his privacy or any other statute, the undersigned finds such arguments unpersuasive and recommends that the District Judge deny them.

CONCLUSION

The undersigned recommends to the District Judge that he deny Defendant's motion to suppress, or in the alternative, Defendant's request for a *Franks* hearing (ECF No. 62). The undersigned further recommends that the District Judge deny Defendant's motion to suppress evidence referenced in the government's notice of intent to use evidence on the basis that such evidence was obtained in violation of various federal privacy statutes (ECF No. 72).

Pursuant to 28 U.S.C. § 636(b)(1), it is hereby

ORDERED, that this Report and Recommendation be filed with the Clerk of the Court.

ANY OBJECTIONS to this Report and Recommendation must be filed with the Clerk of this Court within fourteen (14) days after receipt of a copy of this Report and Recommendation in accordance with the above statute and Rule 59(b) of the Local Rules of Criminal Procedure for the Western District of New York.[7]

The district court will ordinarily refuse to consider on *de novo* review arguments, case law and/or evidentiary material which could have been, but was not, presented to the magistrate judge in the first instance. *See*, *e.g.*, *Paterson-Leitch Co. v. Mass. Mun. Wholesale Elec. Co.*, 840 F.2d 985 (1st Cir. 1988).

Failure to file objections within the specified time or to request an extension of such time waives the right to appeal the District Court's Order. *Thomas v.* Arn, 474 U.S. 140 (1985); *Small v. Sec'y of Health & Human Servs.*, 892 F.2d 15 (2d Cir. 1989); Wesolek *v. Canadair Ltd.,* 838 F.2d 55 (2d Cir. 1988).

The parties are reminded that, pursuant to Rule 59(b) of the Local Rules of Criminal Procedure for the Western District of New York, "[w]ritten objections . . . shall specifically identify the portions of the proposed findings and recommendations to which objection is made and the basis for such objection and shall be supported by legal authority." **Failure to comply with the provisions of Rule 59(b) may result in the District Court's refusal to consider the objection.**

Let the Clerk send a copy of this Order and a copy of the Report and Recommendation to the attorneys for the parties.

IT IS SO ORDERED.

DATED: September 29, 2023
Rochester, New York

MARK W. PEDERSEN
United States Magistrate Judge